(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－79730

(43)公開日　平成10年(1998)３月24日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ａ	
	9/14			Ｈ０４Ｎ	7/16	Ａ	
Ｈ０４Ｎ	7/16			Ｈ０４Ｌ	9/00	６４１	

審査請求　未請求　請求項の数４　ＯＬ　（全６頁）

(21)出願番号　特願平8－233100

(22)出願日　平成８年(1996)９月３日

(71)出願人　396001360
株式会社ディジタル・ビジョン・ラボラトリーズ
東京都港区赤坂七丁目３番37号

(72)発明者　村谷　博文
東京都港区赤坂七丁目３番37号　株式会社ディジタル・ビジョン・ラボラトリーズ内

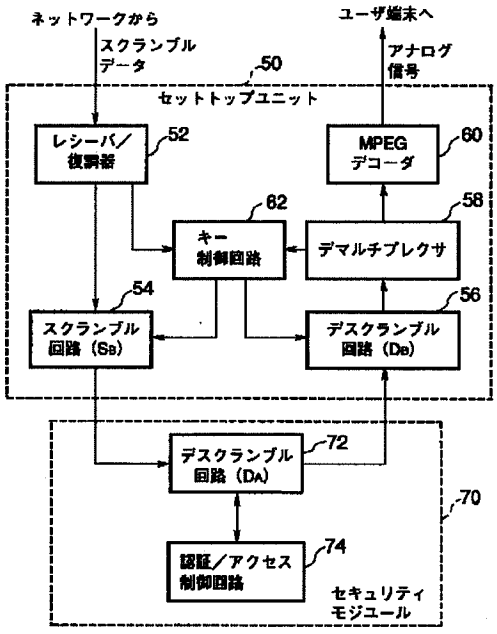
(74)代理人　弁理士　鈴江　武彦　（外５名）

(54)【発明の名称】　復号化装置

(57)【要約】

【課題】本発明はユーザの秘密情報保護と、暗号化データの保護という２つの要求をともに満足する復号化装置を提供することである。

【解決手段】ネットワークから供給され、第１の方式でスクランブルされているディジタル画像データをセットトップユニット５０内のスクランブル回路５４で第２の方式でスクランブル処理し、これをセキュリティモジュール７０へ供給する。セキュリティモジュール７０内では、このデータをデスクランブル回路７２で第１のデスクランブル処理し、セットトップユニット５０へ返送する。このデータはセットトップユニット５０内のデスクランブル回路５６で第２のデスクランブル処理され、ＭＰＥＧデコーダ６０を介して画像表示端末へ出力される。



【特許請求の範囲】
【請求項１】　第１の方式で暗号化されているデータを復号化する復号化装置において、
暗号化データを受信する第１のユニットと、第１のユニットに着脱自在に接続される第２のユニットとを具備し、
前記第２のユニットは前記第１のユニットから供給されたデータを第１の方式で復号化して第１のユニットへ返送する手段を具備し、
前記第１のユニットは受信したデータを第２の方式で暗号化して第２のユニットに出力する手段と、前記第２のユニットから供給されたデータを第２の方式で復号化する手段とを具備することを特徴とする復号化装置。
【請求項２】　前記第１のユニットは第２の方式の暗号化／復号化キーを発生するキー発生手段を具備し、前記キー発生手段から出力されるキー信号は第１のユニットの外部へは出力されないことを特徴とする請求項１に記載の復号化装置。
【請求項３】　前記第２のユニットは第１の方式の復号化キーを記憶しているメモリを具備し、前記メモリから出力されるキー信号は第２のユニットの外部へは出力されないことを特徴とする請求項１に記載の復号化装置。
【請求項４】　前記第１のユニットのキー発生手段から発生される第２の方式の暗号化／復号化キーは可変であることを特徴とする請求項１～請求項３のいずれかに記載の復号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はネットワーク等に接続され、ネットワーク等から供給される暗号化されたデータを復号化する復号化装置に関する。
【０００２】
【従来の技術】近年、ネットワークが発達し、種々の情報サービスが提供されている。サービス提供者は真正の契約者以外の第３者が情報を無償で受信することを防止するために、情報を暗号化してネットワーク上に流す。サービス提供者は契約者のみに復号化キーを知らせ、契約者のみが情報を正しく復号化できるようにしている。なお、情報のサービスは有線のネットワークのみならず、無線ＬＡＮ、テレビジョン放送等においても広く行われている。
【０００３】このような復号化装置の従来例としては、図１に示すような装置がある。この装置は、セットトップユニット１０、セキュリティモジュール２０、ＩＣカード３０からなるが、セットトップユニット１０、セキュリティモジュール２０は実際には一体化され、１つの製品（復号化装置）として実現されている。そして、ＩＣカード３０のみがこの製品とは別体となっている。
【０００４】ネットワーク（無線ＬＡＮ、テレビジョン放送の場合は、アンテナ）から供給された暗号化データ（ここでは、暗号化はスクランブル化とし、以下、暗号化データをスクランブルデータと称する）はセットトップユニット１０のレシーバ／復調器１２に入力される。この例では、オリジナルデータはＭＰＥＧ方式で符号化されているディジタル画像データであるとする。レシーバ／復調器１２の出力（スクランブルデータ）はセキュリティモジュール２０に供給され、デスクランブル回路２２及びフィルタ２４に入力される。
【０００５】フィルタ２４は入力されたストリームデータからＥＣＭとＥＭＭを取り出し、インターフェース２６へ供給する。ＥＣＭとＥＭＭはＭＰＥＧ２において定義されているデータであり、ＥＣＭはEntitlement control message 、ＥＭＭはEntitlement management messageの略である。具体的には、画像や音声データを転送するＭＰＥＧトランスポートストリームのパケットのペイロードがスクランブルされたときに、そのトランスポートストリーム中に流される制御情報を含んだストリームのことである。
【０００６】ＥＣＭには、そのスクランブルを解くために必要な鍵（キー）、プログラム番号（ＭＰＥＧ２ではプログラムとは共通のタイムベースを持った画像・音声データストリームの集まりを意味する）、プログラムの利用料など、その画像・音声データのストリームに固有のアクセス制御のための情報が含まれる。
【０００７】ＥＭＭには、システム全体に関するアクセス制御のための情報が含まれる。例えば、利用者の新規加入や新しいプログラム番号などが含まれる。このように、フィルタ２４は符号化された画像・音声データのストリームに混ざって送られてくるＥＣＭとＥＭＭを含んでいるストリーム（プログラムストリームならば、program stream map、トランスポートストリームならば、TS program map sectionというストリーム）を取り出すためのフィルタリングを行う。このフィルタリングはパケットに割り振られているＰＩＤ（パケットＩＤ）やストリームＩＤの値に応じて行われる。
【０００８】インターフェース２６は契約者が所有するＩＣカード３０に接続される。ディジタル画像データの送信者であるサービス提供者は、送信時のスクランブルに対応したデスクランブルキー、ユーザのパスワード等をＩＣカード３０に予め書き込み、これを契約時にユーザに渡す。
【０００９】図１のシステムでは、復号化装置（セットトップユニット１０、セキュリティモジュール２０からなる）を所有していることが一種の本人認証になるが、装置の盗難等に対処するために、実際にはパスワード照合等の本人認証が行われる。
【００１０】ＩＣカード３０とインターフェース２６が接続され、認証が成功すると、ＩＣカード３０からデスクランブルキーがセキュリティモジュール２０内のデスクランブル回路２２へ入力される。

【００１１】デスクランブル回路２２はこのデスクランブルキーを用いて、セットトップユニット１０から供給されたスクランブルデータをデスクランブルし、オリジナルのＭＰＥＧ符号化ディジタル画像データをセットトップユニット１０へ返送する。オリジナルデータはセットトップユニット１０内のマルチプレクサ１４、ＭＰＥＧデコーダ１６を介して図示しないユーザ端末（画像表示装置等）へ出力される。ＭＰＥＧデコーダ１６はアナログ／ディジタル変換器を内蔵し、オリジナルのアナログ画像信号を出力する。

【００１２】このように、セキュリティモジュール２０によりスクランブルデータのデスクランブルが行われ、オリジナルのＭＰＥＧ符号化ディジタル画像データがセットトップユニット１０に供給される。そのため、真正のユーザのみデスクランブルが可能となる。

【００１３】しかしながら、この復号化装置においては、デスクランブルキー等のユーザの秘密情報がインターフェース２６に現れる。このため、このインターフェースを介してユーザの秘密情報が第３者に盗まれる可能性があり、ユーザ保護、セキュリティの点で問題がある。

【００１４】そこで、これを回避するために、ＩＣカード３０とセキュリティモジュール２０を一体化する（セットトップユニット１０とセキュリティモジュール２０を別体とする）ことも考えられる。この場合は、ユーザの秘密情報が第３者に盗まれることは無くなるが、セキュリティモジュール２０とセットトップユニット１０との間のインターフェースにデスクランブルされたオリジナルのディジタル画像データが現れるので、これを不正に利用（コピー等）される可能性があり、サービス提供者にとって脅威である。なお、上述した問題は、ネットワークを介して供給される情報の復号の際に限られずに、パッケージされたソフトウェアの流通等においても同様に生じる。

【００１５】

【発明が解決しようとする課題】このように従来の復号化装置はユーザの秘密情報保護と、暗号化データの保護という２つの要求をともに満足することは不可能であるという欠点があった。本発明は上述した事情に対処すべくなされたもので、その目的はユーザの秘密情報を保護できるとともに、暗号化データの不正利用を防止できる復号化装置を提供することである。

【００１６】

【課題を解決するための手段】本発明による復号化装置は、第１の方式で暗号化されているデータを復号化する復号化装置において、暗号化データを受信する第１のユニットと、第１のユニットに着脱自在に接続される第２のユニットとを具備し、前記第２のユニットは前記第１のユニットから供給されたデータを第１の方式で復号化して第１のユニットへ返送する手段を具備し、前記第１のユニットは受信したデータを第２の方式で暗号化して第２のユニットに出力する手段と、前記第２のユニットから供給されたデータを第２の方式で復号化する手段とを具備することを特徴とする。

【００１７】また、前記第１のユニットは第２の方式の暗号化／復号化キーを発生する手段を具備し、前記発生手段から出力される信号はユニットの外部へは出力されないことも特徴とする。

【００１８】また、前記第２のユニットは第１の方式の復号化キーを記憶しているメモリを具備し、前記メモリから出力される信号はユニットの外部へは出力されないことも特徴とする。

【００１９】さらに、前記第１のユニットのキー発生手段から発生される第２の方式の暗号化／復号化キーは可変であることも特徴とする。本発明による復号化装置によれば、第１のユニットと第２のユニットとの間のインターフェースには少なくとも第２の暗号化が行われているデータしか現れないので、暗号化データの不正利用が防止できる。

【００２０】また、ユーザの秘密情報は第２のユニットから外部に出力されないので、ユーザの秘密情報も保護できる。また、第２の方式の暗号化／復号化キーは第１のユニットから外部に出力されないので、このキーが第３者に見破られる可能性が非常に小さい。さらに、第２の方式の暗号化／復号化キーは可変であるので、このキーが第３者に見破られる可能性が非常に少ない。

【００２１】

【発明の実施の形態】以下、図面を参照して本発明による復号化装置の第１の実施形態を説明する。図２は第１の実施形態のブロック図である。本実施形態はセットトップユニット５０と、セキュリティモジュール７０からなり、これらは従来例とは異なり、別体とされ着脱自在であり、両者間にインターフェースが存在する。

【００２２】セットトップユニット５０は、レシーバ／復調器５２、スクランブル回路５４、デスクランブル回路５６、デマルチプレクサ５８、ＭＰＥＧデコーダ６０、キー制御回路６２からなる。セキュリティモジュール７０は、デスクランブル回路７２、認証／アクセス制御回路７４からなる。なお、セキュリティモジュール７０はＩＣカードの形として実現してもよい。

【００２３】従来例と同様に、ネットワーク、あるいはアンテナから供給された暗号化データ（スクランブルされているＭＰＥＧディジタル画像データ）はセットトップユニット１０のレシーバ／復調器５２に入力される。スクランブル処理は図示しない情報提供者のサーバ側で行われ、このスクランブル処理を第１のスクランブル処理（S_A）と称する。レシーバ／復調器５２の出力はサーバ側の第１のスクランブル処理（S_A）とは異なる所定の第２のスクランブル処理（S_B）を行うスクランブル回路５４と、第２のスクランブル処理のキーを制御す

るキー制御回路６２に供給される。

【００２４】キー制御回路６２はレシーバ／復調器５２からデータが供給されると、第２のスクランブル処理のためのスクランブルキー、及びこれに対応するデスクランブルキーを発生し、スクランブルキー、デスクランブルキーをスクランブル回路５４、デスクランブル回路５６へそれぞれ供給する。第１、第２のデスクランブル処理をD_A、D_Bとすると、キー制御回路６２は$D_B \cdot D_A \cdot S_B \cdot S_A = I$（Ｉ：単位行列）を満足するような第２スクランブル処理のためのスクランブルキー、デスクランブルキーを発生する。

【００２５】スクランブル回路５４はキー制御回路６２からのスクランブルキーを用いて第２のスクランブル処理（S_B）を行う。スクランブル回路５４の出力がセキュリティモジュール７０に供給され、第１のデスクランブル処理（D_A）を行うデスクランブル回路７２に入力される。

【００２６】デスクランブル回路７２は認証／アクセス制御回路７４から供給されるデスクランブルキーを用いてセットトップユニット５０から供給されたデータに第１のデスクランブル処理（D_A）を行い、デスクランブルデータをセットトップユニット５０に返送する。ディジタル画像データの送信者であるサービス提供者は、送信時の第１のスクランブル処理に対応したデスクランブルキーを認証／アクセス制御回路７４に予め書き込み、これを契約時にユーザに渡す。そのため、デスクランブル回路７２からは、ネットワークからセットとプユニット５０に供給されたデータの第１のスクランブルが解除されたデータが得られる。ただし、このデータには、スクランブル回路５４による第２のスクランブル処理（S_A）は行われている。

【００２７】認証／アクセス制御回路７４は従来のＩＣカードの代わりに、サービス提供者によってデスクランブルキー、ユーザのパスワード等が書き込まれており、これを内蔵したセキュリティモジュール７０を所有することが一種の認証となる。

【００２８】セットトップユニット５０内で、デスクランブル回路５６はキー制御回路６２から供給されるデスクランブルキーを用いて入力データに第２のデスクランブル処理（D_B）を行い、オリジナルのＭＰＥＧ符号化ディジタル画像データを再現する。デスクランブル回路５６の出力がデマルチプレクサ５８、ＭＰＥＧデコーダ６０を介して図示しないユーザ端末（画像表示装置等）へ出力される。ＭＰＥＧデコーダ６０はアナログ／ディジタル変換器を内蔵し、アナログ画像信号を出力する。

【００２９】図３を参照して、本実施形態の動作を説明する。図３はスクランブル処理、デスクランブル処理のみを抽出して示す図であり、ここでは、サーバ４０側の第１のスクランブル処理（ＳＡ）を行う第１のスクランブル回路４２も示している。オリジナルのディジタルデータをＭとすると、サーバ４０内の第１のスクランブル回路４２は、第１の方式でスクランブル処理したデータS_A（Ｍ）を出力する。

【００３０】このデータがセットトップユニット５０で受信されると、第２のスクランブル回路５４はこのデータに第２のスクランブル処理を行い、S_B（S_A（Ｍ））を出力する。このため、セットトップユニット５０からセキュリティモジュール７０へは第１、第２のスクランブル方式で二重にスクランブルされたデータが供給される。このデータは、たとえ第３者に盗まれてもデスクランブルできないので、オリジナルデータを再現することはできず、オリジナルディジタルデータの不正利用の心配はない。

【００３１】セキュリティモジュール７０内の第１のデスクランブル回路７２は、この二重スクランブルデータに第１の方式のデスクランブル処理（D_A）を行い、D_A（S_B（S_A（Ｍ））＝S_B（Ｍ）を出力し、セットトップユニット５０へ返送する。このため、セキュリティモジュール７０からセットトップユニット５０へは第２の方式でスクランブルされたデータが供給される。このデータも、たとえ第３者に盗まれてもデスクランブルできないので、オリジナルデータを再現することはできず、オリジナルディジタルデータの不正利用の心配はない。特に、第２のスクランブル処理のキーはセットトップユニット５０内のキー制御回路６２で発生されるので、外部に漏れることはなく、オリジナルデータの第３者の不正利用を防ぐことができる。

【００３２】セットトップユニット５０内の第２のデスクランブル回路５６は、この入力データに第２の方式のデスクランブル処理（D_B）を行い、D_B（D_A（S_B（S_A（Ｍ））））を出力する。前述したように、キー制御回路６２は第２のスクランブル処理／デスクランブル処理S_B、D_Bが$D_B \cdot D_A \cdot S_B \cdot S_A = I$となるように選ばれているので、$D_B$（$D_A$（$S_B$（$S_A$（Ｍ））））＝Ｍとなり、デスクランブル回路５６はオリジナルデータを再現できる。なお、$D_B \cdot D_A \cdot S_B \cdot S_A = I$ということは、必ずしも、$D_A \cdot S_A = D_B \cdot S_B = I$であることではない。

【００３３】このように、本実施形態によれば、セットトップユニット５０とセキュリティモジュール７０との間のインターフェースには、オリジナルのディジタルデータが現れることがないので、オリジナルディジタルデータの不正利用（コピー等）が不可能であり、サービス提供者の保護が十分できる。さらに、従来のようにＩＣカードとセキュリティモジュールとのインターフェースが存在しないので、パスワード、デスクランブルキー等のユーザの秘密情報が第３者に盗まれることも無い。

【００３４】さらに、セキュリティを高めるために、キー制御回路６２は定期／不定期に第２のスクランブル処理のためのキーを変更するとなお効果的である。すなわ

ち、セットトップユニット５０から出力されるデータをモニタすることにより、第２のスクランブルのキーが見破られてしまう可能性が０ではない。しかし、キーを可変とすることにより、このような可能性を実質的に０とすることができる。

【００３５】なお、セットトップユニット５０とセキュリティモジュール７０とを別体とすることにより、次のような効果がある。セットトップユニット５０を複数の利用者が共有できる。すなわち、家庭に１台のセットトップユニット５０を設置し、家族の各々が固有のセキュリティモジュール７０を所有することもできる。また、サービス提供者によってスクランブル方式が異なることが考えられるが、この場合でも、サービス提供者固有のデスクランブル機能をセキュリティモジュールに組み込むことにより、１台のセットトップユニット５０で対処できる。

【００３６】本発明は上述した実施形態に限定されず、種々変形して実施可能である。例えば、上述の説明では、暗号化はスクランブル化として説明したが、これに限らず、ＲＳＡ方式、ＤＥＳ方式等の通常の暗号化でもよい。また、ネットワークから供給されるデータは画像データに限らず、音声データ、ビデオデータ等でもよい。さらに、データの供給形態はネットワークを介して供給される場合のみならず、記憶媒体を介して供給される場合にも適用可能である。

【００３７】

【発明の効果】以上説明したように本発明によれば、ユーザの秘密情報を保護できるとともに、暗号化データの不正利用を防止できる復号化装置が提供される。

【図面の簡単な説明】

【図１】従来の復号化装置の構成を示すブロック図。

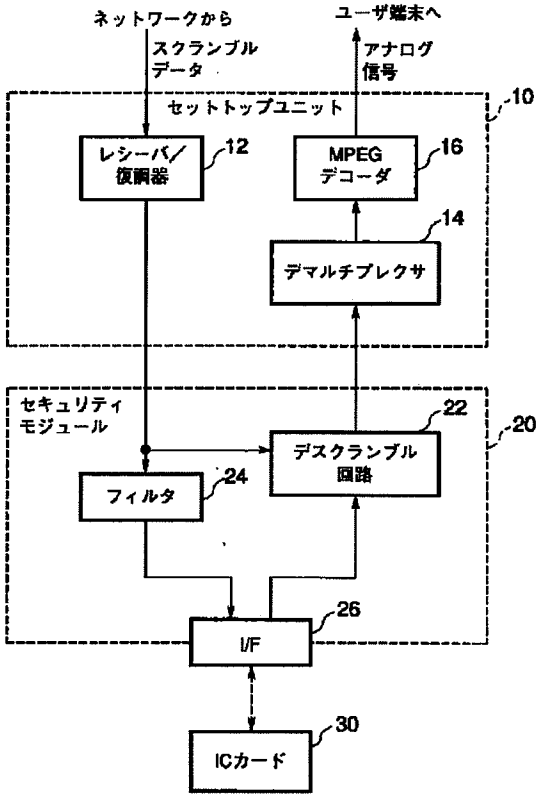
【図２】本発明による復号化装置の第１の実施形態の構成を示すブロック図。

【図３】第１の実施形態のスクランブル・デスクランブル処理を示す概略図。

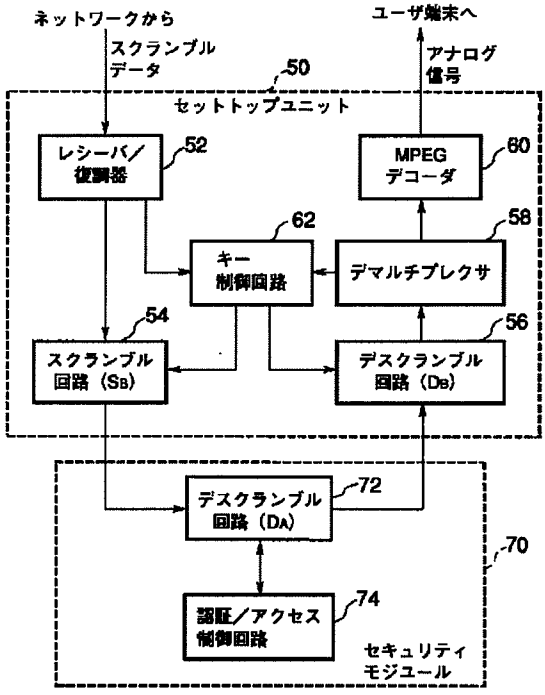
【符号の説明】

４０…サーバ
４２…スクランブル回路（S_A）
５０…セットトップユニット
５４…スクランブル回路（S_B）
５６…デスクランブル回路（D_B）
６０…ＭＰＥＧデコーダ
６２…キー制御回路
７０…セキュリティモジュール
７２…デスクランブル回路（D_A）
７４…認証／アクセス制御回路

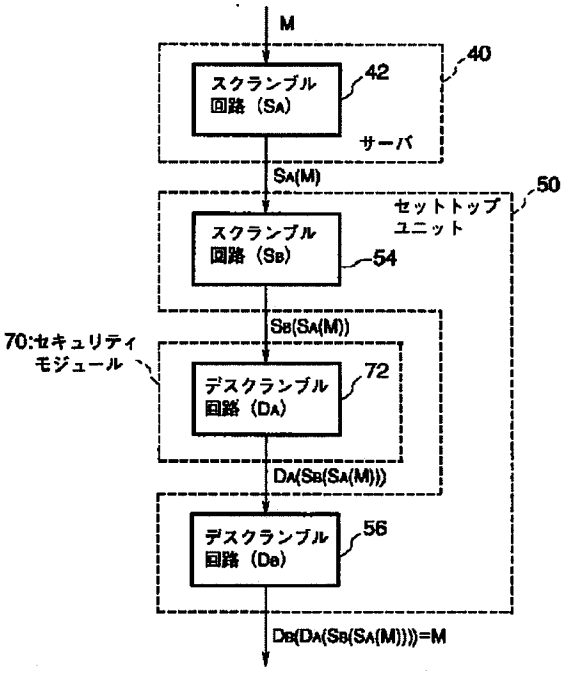
【図１】



【図２】



【図３】


M
スクランブル
回路（SA）
42
40
サーバ
SA(M)
セットトップ
ユニット
50
スクランブル
回路（SB）
54
SB(SA(M))
70:セキュリティ
モジュール
デスクランブル
回路（DA）
72
DA(SB(SA(M)))
デスクランブル
回路（DB）
56
DB(DA(SB(SA(M))))=M

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-079730**
(43)Date of publication of application : **24.03.1998**

(51)Int.Cl. **H04L 9/10**
H04L 9/14
H04N 7/16

(21)Application number : **08-233100** (71)Applicant : **DIGITAL VISION LAB:KK**
(22)Date of filing : **03.09.1996** (72)Inventor : **MURATANI HIROBUMI**

(54) DECODER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a decoder satisfying both of two requirements as secret information protection of user and ciphered data.
SOLUTION: A scramble circuit 54 in a set-top unit 50 applies scramble processing with a 2nd system to digital image fed from a network and scrambled by a 1st systemand the processed data are fed to a security module 70. A descramble circuit 72 of the security module 70 applies 1st descramble processing to the data and returns the result to the set-top unit 50. The data are subjected to 2nd descramble processing by a descramble circuit 50 in the set-top unit 50 and the processed data are outputted to an image display terminal equipment via an MPEG decoder 60.

CLAIMS

[Claim(s)]
[Claim 1]A decoding device which decrypts data enciphered by the 1st methodcomprising:
The 1st unit that receives encryption data.
The 2nd unit connected to the 1st unit enabling free attachment and detachment is providedA means for said 2nd unit to possess a means to decrypt data supplied from said 1st unit by the 1st methodand to return it to the 1st unitand for said 1st unit to encipher received data by the 2nd methodand to output to the 2nd unit.
A means to decrypt data supplied from said 2nd unit by the 2nd method.

[Claim 2]The decoding device according to claim 1wherein a key signal which said 1st unit possesses a key generation means to generate encryption/decryption key of the 2nd methodand is outputted from said key generation means is not

outputted to the exterior of the 1st unit.
[Claim 3]The decoding device according to claim 1wherein a key signal which said 2nd unit possesses a memory which has memorized a decryption key of the 1st methodand is outputted from said memory is not outputted to the exterior of the 2nd unit.
[Claim 4]The decoding device according to any one of claims 1 to 3wherein encryption/decryption key of the 2nd method generated from a key generation means of said 1st unit is variable.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]It is connected to a network etc. and this invention relates to the decoding device which decrypts the enciphered data which is supplied from a network etc.
[0002]
[Description of the Prior Art]In recent yearsa network progresses and various information services are provided. In order to prevent the 3rd person other than a genuine contractor from receiving information gratuitouslya purveyor of service enciphers information and passes on a network. A purveyor of service informs only a contractor of a decryption keyand only the contractor enables it to decrypt information correctly. Service of information is widely offered also not only in the network of a cable but in wireless LANtelevision broadcastingetc.
[0003]As a conventional example of such a decoding devicethere is a device as shown in drawing 1. Although this device consists of the set top unit 10the security module 20and IC card 30actuallyit is unified and the set top unit 10 and the security module 20 are realized as one product (decoding device). And only IC card 30 serves as this product with the different body.
[0004]The encryption data (hereencryption considers it as scramble-ization and calls encryption data scramble data hereafter) supplied from the network (it is an antenna in the case of wireless LAN and television broadcasting) is inputted into the receiver / demodulator 12 of the set top unit 10. In this exampleoriginal data presuppose that it is the digital image data coded with the MPEG system. The output (scramble data) of a receiver / demodulator 12 is supplied to the security module 20and is inputted into the descramble circuit 22 and the filter 24.
[0005]The filter 24 takes out ECM and EMM from the inputted stream dataand supplies them to the interface 26. ECM and EMM are data defined in MPEG 2and Entitlement control message and EMM of ECM are the abbreviation for Entitlement management message. When the scramble of the pay load of the packet of the MPEG transport stream which transmits a picture and voice data is specifically carried outit is the stream included the control information passed in the transport stream.

[0006]A key (key) required for ECM in order to solve the scramblea program number (by MPEG 2a program means the meeting of a picture and a voice data stream with common time base)The information for access control peculiar to the stream of its picture and voice datasuch as a fee of a programis included.
[0007]The information for the access control about the whole system is included in EMM. For examplea user's new enrollmenta new program numberetc. are contained. Thusthe stream containing ECM and EMM which are sent by mixing the filter 24 with the stream of the coded picture and voice data (if it is a program stream) If it is program stream map and a transport streamfiltering for taking out a stream called TS program map section will be performed. This filtering is performed according to the value of PID (packet ID) currently assigned to the packet or stream ID.
[0008]The interface 26 is connected to IC card 30 which a contractor owns. The purveyor of service who is a sending person of digital image data writes beforehand the password of the descrambling key corresponding to the scramble at the time of transmissionand a useretc. in IC card 30and hands this to a user at the time of a contract.
[0009]the person himself/herself of a kind [own / in the system of drawing 1 / the decoding device (it consists of the set top unit 10 and the security module 20)] -- although it is attestedin order to cope with the theft of a deviceetc. -- actual -- the persons themselves himself/herselfsuch as a password examination-- attestation is performed.
[0010]If the interface 26 is connected with IC card 30 and attestation is successfula descrambling key will be inputted into the descramble circuit 22 in the security module 20 from IC card 30.
[0011]The descramble circuit 22 descrambles the scramble data supplied from the set top unit 10 using this descrambling keyand returns original MPEG coding digital image data to the set top unit 10. Original data are outputted to the user terminals (image display device etc.) which are not illustrated via the multiplexer 14 in the set top unit 10and MPEG decoder 16. MPEG decoder 16 builds in an analog-to-digital conversion machineand outputs an original analog picture signal.
[0012]Thusdescrambling of scramble data is performed by the security module 20and original MPEG coding digital image data is supplied to the set top unit 10. Thereforeit becomes possible [descrambling] only for a genuine user.
[0013]Howeverin this decoding devicethe confidential information of userssuch as a descrambling keyappears in the interface 26. For this reasona user's confidential information may be stolen by the 3rd person via this interfaceand there is a problem in respect of user protection and security.
[0014]Thenin order to avoid thiswhat (let the set top unit 10 and the security module 20 be different bodies) IC card 30 and the security module 20 are unified also for is considered. In this casealthough it is lost that a user's confidential information is stolen by the 3rd personSince the original digital image data descrambled by the interface between the security module 20 and the set top unit 10 appearsthis may be used unjustly and it is a threat to a purveyor of service

(copy etc.). The problem mentioned above is similarly produced in circulation etc. of the packed softwarewithout being restricted in the case of decoding of the information supplied via a network.
[0015]
[Problem(s) to be Solved by the Invention]Thusthe conventional decoding device had the fault that it was impossible to satisfy both two demands called a user's confidential information protection and protection of encryption data. While this invention was made that the situation mentioned above should be coped with and the purpose can protect a user's confidential informationit is providing the decoding device which can prevent the illegal use of encryption data.
[0016]
[Means for Solving the Problem]As for a decoding device by this inventionthis invention is characterized by that a decoding device which decrypts data enciphered by the 1st method comprises the following.
The 1st unit that receives encryption data.
The 2nd unit connected to the 1st unit enabling free attachment and detachment is providedA means for said 2nd unit to possess a means to decrypt data supplied from said 1st unit by the 1st methodand to return it to the 1st unitand for said 1st unit to encipher received data by the 2nd methodand to output to the 2nd unit.
A means to decrypt data supplied from said 2nd unit by the 2nd method.

[0017]Said 1st unit possesses a means to generate encryption/decryption key of the 2nd methodand a signal outputted from said generating means is characterized also by not being outputted to the exterior of a uniteither.
[0018]Said 2nd unit possesses a memory which has memorized a decryption key of the 1st methodand a signal outputted from said memory is characterized also by not being outputted to the exterior of a uniteither.
[0019]Encryption/decryption key of the 2nd method generated from a key generation means of said 1st unit is characterized also by being variable. Since only data in which 2nd encryption is performed at least appears in an interface between the 1st unit and the 2nd unit according to the decoding device by this inventionan illegal use of encryption data can be prevented.
[0020]Since a user's confidential information is not outputted outside from the 2nd unita user's confidential information can also be protected. Since encryption/decryption key of the 2nd method is not outputted outside from the 1st unitits a possibility that this key will be detected by the 3rd person is dramatically small. Since encryption/decryption key of the 2nd method is variablethere are dramatically few possibilities that this key will be detected by the 3rd person.
[0021]
[Embodiment of the Invention]Hereafterwith reference to drawingsa 1st embodiment of the decoding device by this invention is described. Drawing 2 is a block diagram of a 1st embodiment. This embodiment serves as the set top unit 50 from the security module 70and unlike a conventional examplethese are made into

a different bodyit can detach and attach freelyand an interface exists among both.
[0022]The set top unit 50 consists of a receiver / demodulator 52the scramble circuit 54the descramble circuit 56the demultiplexer 58MPEG decoder 60and the key control circuit 62. The security module 70 consists of the descramble circuit 72and the attestation/access control circuit 74. The security module 70 may be realized as a form of an IC card.
[0023]The encryption data (MPEG digital image data by which scramble is carried out) supplied from the network or the antenna is inputted into the receiver / demodulator 52 of the set top unit 10 like a conventional example. Scramble processing is performed by the server side of the information provider who does not illustrateand calls this scramble processing the 1st scramble processing (S_A). The output of a receiver / demodulator 52 is supplied to the scramble circuit 54 which performs the 2nd different predetermined scramble processing (S_B) from the 1st scramble processing (S_A) by the side of a serverand the key control circuit 62 which controls the key of the 2nd scramble processing.
[0024]If data is supplied from a receiver / demodulator 52the key control circuit 62The scramble key for the 2nd scramble processing and the descrambling key corresponding to this are generatedand a scramble key and a descrambling key are supplied to the scramble circuit 54 and the descramble circuit 56respectively. If the 1st and 2nd descrambling processing is made into D_A and D_BThe key control circuit 62 generates the scramble key for the 2nd scramble processing with which it is satisfied of $D_BD_AS_B$and S_A=I (I: identity matrix)and a descrambling key.
[0025]The scramble circuit 54 performs the 2nd scramble processing (S_B) using the scramble key from the key control circuit 62. The output of the scramble circuit 54 is supplied to the security module 70and it is inputted into the descramble circuit 72 which performs the 1st descrambling processing (D_A).
[0026]The descramble circuit 72 performs the 1st descrambling processing (D_A) to the data supplied from the set top unit 50 using the descrambling key supplied from attestation / access control circuit 74and returns descrambling data to the set top unit 50. The purveyor of service who is a sending person of digital image data writes beforehand the descrambling key corresponding to the 1st scramble processing at the time of transmission in attestation / access control circuit 74and hands this to a user at the time of a contract. Thereforethe data in which the 1st scramble of a set and the data supplied to PUYUNITTO 50 was canceled of the network is obtained from the descramble circuit 72. Howeverthe 2nd scramble processing (S_A) by the scramble circuit 54 is performed to this data.
[0027]Instead of the conventional IC cardthe password of the descrambling key and the useretc. are written in by the purveyor of serviceand attestation / access control circuit 74 serves as attestation of a kind [own / the security module 70 which contained this].
[0028]Within the set top unit 50the descramble circuit 56 performs the 2nd descrambling processing (D_B) to input data using the descrambling key supplied from the key control circuit 62and reproduces original MPEG coding digital image data. It is outputted to the user terminals (image display device etc.) which the

output of the descramble circuit 56 does not illustrate via the demultiplexer 58 and MPEG decoder 60. MPEG decoder 60 builds in an analog-to-digital conversion machineand outputs an analog picture signal.

[0029]Operation of this embodiment is explained with reference to drawing 3. Drawing 3 is a figure extracting and showing only scramble processing and descrambling processingand also shows here the 1st scramble circuit 42 that performs the 1st scramble processing (SA) by the side of the server 40. If original digital data is set to Mthe 1st scramble circuit 42 in the server 40 will output data S_A (M) which carried out scramble processing by the 1st method.

[0030]If this data is received by the set top unit 50the 2nd scramble circuit 54 will perform the 2nd scramble processing to this dataand will output S_B (S_A (M)). For this reasonthe data by which scramble was doubly carried out with the 1st and 2nd scrambling system is supplied to the security module 70 from the set top unit 50. Since this data cannot be descrambled even if it is stolen by the 3rd personoriginal data cannot be reproduced but there are no worries about the illegal use of original digital data.

[0031]The 1st descramble circuit 72 in the security module 70Descrambling processing (D_A) of the 1st method is performed to this double scramble dataD_A(S_B (S_A (M))) =S_B (M) is outputtedand the set top unit 50 is returned. For this reasonthe data by which scramble was carried out by the 2nd method is supplied to the set top unit 50 from the security module 70. Since this data cannot be descrambledeithereven if it is stolen by the 3rd personoriginal data cannot be reproduced but there are no worries about the illegal use of original digital data. Since it is generated in the key control circuit 62 in the set top unit 50the key in particular of the 2nd scramble processing cannot leak outsideand can prevent the illegal use of the 3rd person of original data.

[0032]The 2nd descramble circuit 56 in the set top unit 50 performs descrambling processing (D_B) of the 2nd method to this input dataand outputs D_B (D_A (S_B (S_A (M)))). Since the key control circuit 62 is chosen so that the 2nd scramble processing / descrambling processing $S_B$and D_B may be set to $D_BD_AS_B$and S_A=I as mentioned aboveIt is set to D_B(D_A (S_B (S_A (M)))) =Mand the descramble circuit 56 can reproduce original data. $D_BD_AS_B$andS_A=I is not necessarily $D_A$andS_A=$D_B$andS_B=I.

[0033]Thusaccording to this embodimentfor the interface between the set top unit 50 and the security module 70. Since original digital data does not appearthe illegal uses (copy etc.) of original digital data are impossibleand a purveyor's of service protection can be performed enough. Since the interface of an IC card and a security module does not exist like beforethe confidential information of userssuch as a password and a descrambling keyis not stolen by the 3rd person.

[0034]In order to raise securityin additionthe key control circuit 62 is effectiveif the key for the 2nd scramble processing is changed into a commuter's ticket/stage amphiboles. That isa possibility that the key of the 2nd scramble will be detected is not 0 by monitoring the data outputted from the set top unit 50. Howeversuch a possibility can be substantially set to 0 by making a key variable.

[0035]There are the following effects by using the set top unit 50 and the security

module 70 as a different body. Two or more users can share the set top unit 50. That isone set of the set top unit 50 can be installed in a homeand the security module 70 with a family's peculiar each can also be owned. Although it is possible that a scrambling system changes with purveyors of serviceit can be coped with by one set of the set top unit 50 by including a descrambling function peculiar to a purveyor of service in a security module even in this case.

[0036]This invention is not limited to the embodiment mentioned abovebut changes variouslyand is feasible. For examplein above-mentioned explanationalthough encryption was explained as scramble-izingencryption usual [such as not only this but a RSA methoda DES methodetc.] may be sufficient as it. Not only image data but voice dataa video dataetc. may be sufficient as the data supplied from a network. The supplying form of data can be applied not only when supplied via a networkbut when supplied via a storage.

[0037]

[Effect of the Invention]As explained abovewhile being able to protect a user's confidential information according to this inventionthe decoding device which can prevent the illegal use of encryption data is provided.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The block diagram showing the composition of the conventional decoding device.

[Drawing 2]The block diagram showing the composition of a 1st embodiment of the decoding device by this invention.

[Drawing 3]The schematic diagram showing the scramble descrambling processing of a 1st embodiment.

[Description of Notations]

40 -- Server
42 -- Scramble circuit (S_A)
50 -- Set top unit
54 -- Scramble circuit (S_B)
56 -- Descramble circuit (D_B)
60 -- MPEG decoder
62 -- Key control circuit
70 -- Security module
72 -- Descramble circuit (D_A)
74 -- Attestation/access control circuit